ACCESS CONTROL OF WEB SERVICES USING GENETIC ALGORITHMS

Nabila SEMMACHE and Sadika SELKA
Department of Computer Science
University of The Science And The Technology,
1505-El-Mnouar, Oran, ALGERIA
E-mail: Semmache_hanane@yahoo.fr

KEYWORDS
Web service, SOAP, UDDI, WSDL, WS-Security, Genetic Algorithm.

ABSTRACT

Although Web services have been simplified a lot in terms of development, the problem of the security of these services is crucial and remains still confusing and complex. This last one lies around three axes: the Identification and the authenticity of a user, Protection of the confidential data and the authorization of access to applications of the web services. In this article, among the three axes we are interested in the authorization of access of the users to the applications of the Web services. For that purpose, we propose an approach based on genetic algorithms, so that the tasks of the Web services are secured.

INTRODUCTION

Web service can be defined as a mechanism of communication between distant applications through the Internet network, independent of any programming language and any platform of execution. It is based on standard Web protocols such as XML (*eXtensible Markup Language*), for the coding of the parameters and the values of return, SOAP (*Simple Object Access Protocol*) (Gudgin et al. 2007), for the transport of messages, WSDL(*Web Description Language services*) (Chinnici et al. 2007) for the description and UDDI (*Universal Description, Discovery and Integration*) (Clément et al. 2005) for the publication.

Although these protocols allow today to build applications and to put them in production, numerous evolutions remain to be brought to offer the consideration of quality criteria of services such as protected from delivery, the transactions and the security.

These last years, the research in the field of Web services was very active. A big part of this one was dedicated to the security.

One of the solutions proposed to secure Web services was to assure the reliability of the connection between the customer and the server. With a transport secured as SSL(*Secure Sockets Layer*), (Freier and Karlton 1996) the services do not have to manage themselves the integrity and the confidentiality of every message; they need to relay on the mechanisms of the layer transport underlying. However, they turn out that a security at the level transport (Merrells 2004) is a limited solution to exchanges of messages from a point to the other one.

For this security at the level message (Merrells 2004) was proposed to maximize the reach of the Web services. The standards of security used at this level are: WS-Security (Atkinson et al. 2002), WS-Trust (Della-Libera et al. 2002), WS-Privacy (Nagaratnam et al. 2003), WS-Policy (Curbera et al. 2003), WS-Federation (Bajaj et al. 2003), WS-SecureConversation (Dixon et al. 2002) and WS-Authorization (Della-Libera et al. 2002).

In this article, we propose another security at the level of the tasks of the Web services by using the genetic algorithms, with the aim of controlling the access of the users.

ARCHITECTURE OF WEB SERVICES

The efforts of research and development about Web services led to a number specifications which define the architecture of the Web services (McCabe et al. 2004).

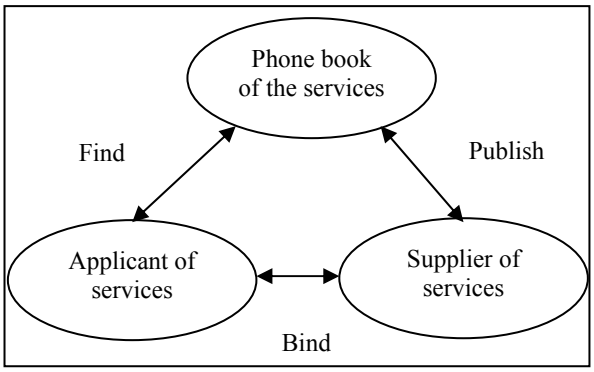

Figure 1 : Architecture of Web services

The architecture of the Web services articulates around the following three roles:

Proceedings of the 2008 High Performance
Computing & Simulation Conference ©ECMS
Waleed W. Smari (Ed.)
ISBN: 978-0-9553018-7-2 / ISBN: 978-0-9553018-6-5 (CD)

- Supplier of service: corresponds to the owner of the service. From a technical point of view, it is constituted by the platform of reception of the service;

- Applicant of service: corresponds to the applicant of service. From a technical point of view, it is constituted by the application which is going to look for and to call upon a service;

- The phone book of the services: corresponds to pad of descriptions of services offering opportunities of publication of services for the suppliers as well as opportunities of research for services for the customers.

ARCHITECTURE OF SECURITY OF WEB SERVICES

For to secure Web services, several mechanisms must be addresses so as to guarantee the security of the exchanges of information:

- The authenticity: allows to verify that the access to an application or to a distant resource is made only by entities having proved their identity;

- The integrity: allows to verify that the message received by the addressee was not modified during its transmission;

- The confidentiality: allows to verify that the transmitted messages cannot be read by entities others than the receiver and the transmitter of the message;

- The non-repudiation: guarantees to the addressee of a message that the transmitter of that this is well the one that it claims to be;

- Authorization of access: put at the disposal of mechanisms allowing to authorize or not the access to such or such resource.

The standards of security used at the level message and that allow to assure these various mechanisms, are illustrated in the figure 2;

<table>
<tr><td>WS-Secure Conversation</td><td>WS-Federation</td><td>WS-Authorization</td></tr>
<tr><td>WS-Policy</td><td>WS-Trust</td><td>WS-Privacy</td></tr>
<tr><td colspan="3">WS-Security</td></tr>
<tr><td colspan="3">Fondation SOAP</td></tr>
</table>

Figure 2 : Architecture of security of web services

- WS-security: Specification of secured messaging using SOAP messages. It processes the following three aspects:

1. Specification of mechanisms allowing to assure the integrity of messages SOAP. It deals more particularly as the joint use of the specification XML signature (Bartel et al. 2002) and as the tokens of security.

2. Specification of mechanisms allowing to assure the confidentiality of messages SOAP. It deals more particularly as the joint use of the specification XML encryption (Takeshi et al. 2002) and as the tokens of security.

3. Definition of a mechanism to associate tokens of security with the headings of messages SOAP. Without recommending of specific format, it specifies a method to create new formats of tokens of security as well as mechanism of encoding of binary tokens.

- WS-Policy: allows describing in terms of security the requirements of the addressee as well as the capacities of security of the transmitter of a message.

- WS-Trust: describes a model allowing establishing reliable relations which can base itself on a system of tokens of security.

- WS-Privacy: describes the policies of discretion and confidentiality.

- WS-Secure Conversation: describes how two entities can communicate by authenticating mutually and by forming a context of security.

- WS-Federation: allows building global reliable spaces so allowing making authenticity between entities using different methods of authenticity.

- WS-Authorization: describes how to manage and to create rules of authorization, to certify authorizations via tokens, to exchange these tokens and to interpret these so as to control correctly the accesses to the services.

SECURITY OF WEB SERVICES USING GENETIC ALGORITHMS

In this article, we are interested in the security of the Web services at the task level to control the access of the users by using genetic algorithms (Rennard 2002). The approach which we propose consists of two phases: phase of discovery and phase of optimization which is really the genetic process.

Phase Of Discovery

A supplier implements Web service, he defines his description in the form of a file WSDL and publishes it by saving it in a phone book UDDI. The example which follows will be studied throughout the article.

Let us consider the case of a travel agency which offers Web service of grouped booking combining a plane ticket, a booking of hotel room and a rent of car among others. For that purpose, the agency calls Web services of an airline company, a hotel chain and a renter out of automobiles.

Here are the tasks executed by every Web service:

- The task executed by Web service of an airline company is: the booking of ticket;

- The task executed by Web service of a chain of hotel is: the booking of room;

- The task executed by Web service of a renter out of automobiles is: the rent of car.

The Parameters of every task, described in WSDL are:

- The parameters of the task booking of ticket: family name, first name, date of departure, date of exit, Country of destination;

- The parameters of the task booking of room: family name, first name, dates of the beginning of stay, Dates of the end of stay, type of room to be reserved;

- The parameters of the task rent of car: family name, first name, dates of the beginning of rent, Dates of the end of rent, Type of car to be rented.

All these parameters will be added to the other parameters which are not described in the file WSDL. For example for the spot of booking of tickets the parameters which will be posted (shown) in WSDL are: family name, first name, and date of departure, date of exit and country of destination. Those which are non-visible are: the number of passport and number of the ID card. After the discovery of the Web services, the phase of optimization follows.

Phase Of Optimization

This phase is the release of the genetic process by the supplier during the invocation of Web service by the customer for the access control of this last one. This genetic process passes by:

- A coding of individuals

- The generation of initial population

All the specific parameters in every task of Web service, supplied by the supplier, are set of individuals which represent the potential solutions to control the access of the users.

Coding Of Individuals

The coding which we propose for our approach is illustrated in table below follows;

Table 1: Table Recapitulating the Correspondences between Main Terminologies of the Genetic Algorithms and Web Services

Natural notion	Definition	Coding of Individuals
Chromosome	One or several chromosomes form together the global genetic plan for the construction and the functioning of a body	The tasks of the Web services
Genes	We say that chromosomes are constituted by genes	The parameters of the tasks of Web services
Alleles	A gene can set different alleles	The Value of every parameter
Locus	The position of a gene	The position of the parameter

The generation of the initial population is made according to two stages: evaluation of the parameters of the initial population and Application of the genetic operators.

Evaluation Of The Parameters Initials

To estimate a specific parameter for a task of Web service, we choose first of all parameters Pi with i € [1, n]. Every parameter will have a value Vij with j € [1, m], determining its degree of importance by contribution to the other parameters chosen. This value is calculated as follows:

$$Vij = Xi / \sum_{i=1}^{n} NbrPi \qquad (1)$$

Vij**:** value j of the parameter i;
Xi: The number of position of the parameter i;
NbrPi : The number of parameters Pi chosen as a task;

For every parameter, we attribute a weight of reliability Pfi with $0 < Pfi < 1$ and i € [1, n], corresponding at the request of access of the users (0 corresponds to 0 % and 1 corresponds to 100 %). This means that this weight of reliability Pfi, changes according to the demand of access of the users.

In a general way, the function of adaptation measures the performance of an individual in the resolution of the problem posed. In the precise context of the problem of access controlling, the adaptation of every specific parameter to a task of Web services, is expressed in our approach as follow:

$$F(Pi) = Vij \sum_{i=1}^{n} Pfi \qquad (2)$$

According to the previous example of the travel agency, table2 illustrates the values of the function of adaptation of the parameters of the task “booking of a ticket".

Table 2: Adaptation values of parameters of The ticket booking task

Parameters	Individuals	Values of F(Pi)
Family name	I_1	0.18
First name	I_2	0.20
Country of destination	I_3	0.33
Date of departure	I_4	0.42
Date of exit	I_5	0.56
Number of the ID card	I_6	0.75
Number of passport	I_7	0.80

Genetic Operators

Selection

After calculation of the value of adaptation of every specific parameter to a task of Web services, the operation of selection which is going to allow us to select the potential parameters for access controlling intervenes.

For our approach, the method of chosen selection is elitism. This method of selection allows selecting the best individuals of the population. It is thus the most potential parameters which are going to participate in the improvement of our population.

In our frame of application, the method of selection is translated as follow: the value of the function of adaptation of every parameter will be compared with a called indication "Indication of reliability" Pa, to attribute to every task of Web services.

We fix Pa to a value equal to 0.5, corresponding to 50%. All the parameters which will have a value of adaptation superior or equal to this value (Pa=0.5), will be selected.

According to table 2, the selected parameters are:

{(I_5,0.56) ; (I_6,0.75) ; (I_7,0.80)}

When the potential parameters are selected, we proceed in their mutation.

Mutation

For a better generation, we used another genetic operator “The Mutation ". The method of mutation

which we propose consists of a permutation of two parameters. We are certain that the mutated parameters will always have the shape of a potential solution because we change only the order of the parameters. This permutation is made by basing itself on the value of adaptation of both parameters in the new intermediate generation. What means that among the selected parameters, the one which has the best value of adaptation will be generated.

According to the selected parameters, the mutation is as follows:

$\{(I_6,0.75) ; (I_5,0.56) ; (I_7,0.80)\}$.

APPLICATION OF GENETIC PROCESS

According to the example of the travel agency, we make a case study for a hostile customer who would like to make a booking of a ticket.

The customer calls upon Web service of the booking of ticket by authenticating. There is a start of the genetic process. Two cases appear:

First Case (At Least A Parameter In Wsdl)

Among the generated potential parameters, there is at least a parameter**,** which is at the level of the WSDL elaborated by the supplier. For example for the task of booking of tickets, a generated potential parameter is the date of exit. Thanks to this parameter we control the user.

Here also there are two cases which appear:

The user reaches for the first time thus there are no other parameters which are displayed except those in WSDL. The user is going to make his booking.

The user is authentic, but he wants to modify his date of departure. Since this parameter is potential, another potential parameter, which is not in WSDL, will be displayed, for example, the number of passport.

- If the number of passport is valid: the modification is accepted and the access is authorized.

Let us consider a hostile user who wants to reserve the ticket using the name of somebody else who has already reserved.
For example if he wants to modify the date of departure and it is a potential parameter, then there is a display of another potential parameter which is not in WSDL. For example number of passport. Two cases exist:

- If the number of passport is not valid: the modification is rejected, and so the access is interrupted.
- If the number of passport is valid: the modification is accepted, and the access is authorized.

If in this last case, the customer is suspicious we can control this thanks to another Web service. For example, when he wants to pay the expenses of the ticket (with the banking service), potential parameters appropriate for this service, will be displayed. For example if the entered number of bank card is not valid and if it is a potential parameter, then, there will be a display of another parameter which is the digital signature.

The second case (no potential parameters in WSDL): The control is made by the others Web services.

The last case: if the customer enters with another login, and he does not make his reservation using the name of another person we consider him as an authentic user until the first mistake which he will make.

CONCLUSION

In this article, we proposed an approach of access control of the users in Web services, based on the genetic algorithms. While trying to generate potential parameters among those supplied by the supplier, so that we can demonstrate that from these last ones, the tasks of Web service, can themselves control the access: compound Web services and that of the users.

The purpose of WS-Authorization is to describe how access policies for a Web service are specified and managed. In particular, the goal is to describe how claims may be specified within security tokens and how these claims will be interpreted at the end point.

Thus with WS-authorization, the access control in Web service is made by verifying constraints attributed to the specific parameters of Web services tasks.

With regard to our approach, the access control is made without attribution of constraints for the parameters, the

customer just has to touch a potential parameter generated by the genetic process and described in the file WSDL so that the control begins.
The second advantage is that in WS-authorization, if the supplier adds a parameter, he has to specify ways of access to this new parameter. For our approach, if the supplier adds parameters, it is enough to activate the genetic process to generate new potential parameters and the security starts.

As a perspective of this work, it would be interesting to take into account the profiles of the users.

REFERENCES

Atkinson .B, S. Hada and P. Hallam-Baker. April 2002. “Web Services Security (WS-Security)Version1.0”.

Bajaj .S, B. Dixon and C. Kaler. July 2003. “Web Services Federation Language” .

Bartel .M, J. Boyer, B. Fox and B. LaMacchia. 2002. “Signature Syntax and Processing”.

Chinnici .R, J. Moreau, A. Ryman and S. Weerawarana. June 2007. “Web Services Description Language (WSDL) Version 2.0”.

Clément .L, A. Hately, C. Riegen and T. Rogers, february 2005. “Universal Description Discovery and Integration (UDDI) Version 3.0”.

Curbera .F, D. Langworthy and M. Nottingham. May 2003. “Web Services Policy Framework” .

Della-Libera .G, M. Hondo and P. Hemma. December 2002. “Web Services Trust Language”.

Dixon .B, H. Maruyama and R. Zolfonoon. December 2002. “Secure Web Services Conversation Language”.

Freier .O and P. Karlton. March 1996. “The SSL Protocol Version 3.0”.

Gudgin .M, M. Hadley, N. Mendelsohn, J. Moreau, HF. Nielsen, A. Karmarkar and Y. Lafon. April 2007. “Simple Object Access Protocol (SOAP) Version 1.2”.

Merrells .J. November 2004. “Web Services Security : Access Control”.

McCabe .F, E. Newcomer and M. Champion. February 2004. “Web Services Architecture”.
Nagaratnam .N, M. Hondo and A. Nadalin. June 2003. “Securing Web Services”.

Takeshi .I, D. Blair and E. Simon. 2002. “Encryption Syntax and Processing”.